AO 106 (Rev. 5/85) Affidavit for Search Warrant

United States District Court

DISTRICT OF Delaware

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

[redacted]
Camden-Wyoming, DE 19934,
described more particularly
on Attachment A

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 07-27M

I Taneka Harris being duly sworn depose and say:

I am a(n) FBI Special Agent and have reason to believe
Official Title

that ☐ on the person of or ☒ on the premises known as (name, description and/or location)

[redacted], Camden-Wyoming, DE 19934, described more particularly on Attachment A

in the District of Delaware
there is now concealed a certain person or property, namely (describe the person or property)

see Attachment B

which is (give alleged grounds for search and seizure under Rule 41(b) of the Federal Rules of Criminal Procedure)

contraband and evidence of a crime

in violation of Title 18 United States Code, Section(s) 2252A

The facts to support the issuance of a Search Warrant are as follows:

see attached affidavit

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

Taneka Harris
Signature of Affiant
SA Taneka Harris, FBI

Sworn to before me, and subscribed in my presence

2/9/07 at Wilmington, DE
Date City and State

Honorable Mary Pat Thynge
District Court Magistrate Judge
Name and Title of Judicial Officer

M. Pat Thynge
Signature of Judicial Officer

ATTACHMENT A

LOCATION TO BE SEARCHED

The location of [redacted], Camden, Delaware 19934, can be described as a two-story home with sand-colored siding, green shutters, two-car garage, small front porch, partial stone front, and an open back yard.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Images of child pornography, as defined in 18 U.S.C. § 2256(8), and child erotica, in any format or medium, whether digital, computer file, video tape, film, magazine, or otherwise, including but not limited to the following computer files:

Houston Pictures

a. [redacted]

b. [redacted].jpg

c. [redacted].jpg

d. [redacted].jpg

e. [redacted].jpg

Indianapolis Pictures

a. [redacted].jpg

b. [redacted]jpg

c. [redacted].jpg

d. [redacted]jpg

e. [redacted]jpg

2. Documents and records, in any format, regarding the receipt and/or distribution of child pornography, including the ten computer files listed above.

3. Computers, computer hardware, computer manuals, and related documentation, computer passwords and data security

devices that may be, or are used to visually depict child pornography or child erotica.

4. Computer software, including programs to run operating systems, applications (such as word processing and graphics), utilities and communication programs, including, but not limited to LimeWire and Google "hello" by Picasa P2P softwares.

5. Indicia of occupancy of [redacted], Camden, Delaware 19934, including but not limited to mortgage documents, rental and lease agreements, utility bills, keys, and postmarked mailings.

6. Indicia of subscription to Internet Service Providers, including Comcast residential high speed Internet service, Account No. [redacted]

7. Documents and records in any format, regarding the use of email screen names: [redacted]", "[redacted]", and [redacted]

8. All email correspondence with screen name "[redacted]".

THE UNITED STATES DISTRICT COURT FOR THE

DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF: THE PREMISES KNOWN AS [redacted] Camden-Wyoming, Delaware 19934	)	Case No. _____

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Taneka S. Harris, a Special Agent with the Federal Bureau of Investigation (FBI), Baltimore Division, Wilmington, Delaware Resident Agency, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI since October 31, 2004, and am currently assigned to the Baltimore Division, Wilmington, Delaware Resident Agency. Since joining the FBI, I have been involved in the investigation of bank fraud, terrorism activity, computer intrusion, extortion, and child pornography. Since December 2005, I have been assigned to investigate Crimes Against Children that include the Sexual Exploitation of Children (SEOC) violations of federal law. I have gained expertise in how to conduct such investigations through training classes and everyday work related to conducting these types of investigations. I have attended the Innocent Images National Initiative Undercover Internet Training, Advanced

Innocent Images Training, and the 18th Annual Crimes Against Children Conference.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I am investigating the activities of a computer having internet connection with a service and billing address of [redacted] Camden-Wyoming, Delaware 19934. As will be shown below, there is probable cause to believe that someone using a computer at the above listed address has received, possessed, and/or transmitted child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I am submitting this Affidavit in support of a search warrant authorizing a search of the residence located at [redacted] Camden-Wyoming, Delaware 19934, (the "Premises"), for the items specified in Attachment A. I am requesting authority to search the entire Premises, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment A may be found, and to seize all items listed in Attachment A as instrumentalities, fruits, and evidence of crime.

4. All information contained in this affidavit is either personally known to the affiant or has been related to the affiant by other Special Agents of the Federal Bureau of

Investigation and Detectives with the Indiana State Police. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, U.S.C. §§ 2252 and 2252A, are presently located at the Premises.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252, relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce. 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in

interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment A to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict

access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which preform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap"

protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers,

Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTER AND CHILD PORNOGRAPHY

7. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

8. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With digital cameras the images can be transferred

directly onto a computer. A computer can connect to another computer through the use of telephone, cable, or wireless connections. Electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used,

however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

14. A growing phenomenon on the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of

digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Limewire, one type of P2P software, sets up its searches by keyword. The results of the keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

15. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed of the file(s) he/she wants to download. The file is downloaded directly from the computer hosting the file. The downloaded file is stored in the area previously designated by the user. The downloaded file will remain there until moved or deleted.

16. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a Limewire user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a Limewire user downloading an image file receives the entire image from one computer.

17. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

18. The P2P method resolved the limitations related to file size and attachment size restrictions. However, the typical P2P method is not secure, and unless steps are taken by the offender with contraband files to share, they can be identified and prosecuted. Additionally, the P2P method does not facilitate actual communication between the parties trading the files. Third party software is available to identify the IP address of the P2P computer sending the file and to identify if parts of the

file came from one or more IP addresses. Such software monitors and logs Internet and local network traffic.

19. Google's "hello" software program by Picasa may be the newest answer for individuals trading child pornography and wishing to build a support network and rapport among individual traders. The program lets traders connect directly (P2P) to each other's computers, specifically for the purpose of sharing pictures. Movie files may also be shared but in a limited fashion. Since the connection is P2P, there is no limit to the number and size of pictures that may be shared. Once a connection is created, the individuals simply select the pictures they wish to share. This may be an individual picture or a folder containing thousands of pictures. While connected, the individuals may also engage in chat. All pictures and chats are encrypted during the transmission by the software.

20. When a user selects to send pictures, a dialog box will open. The dialog box will display the default path to send pictures from on the local user's computer. The local user can also navigate to any other path to select a different location where the image may be sent.

21. The only downside to the use of the program is the lack of a search feature to locate and identify other "hello" users. The traders must learn each other's handles (also frequently referred to as a screen name or user name) by other methods such

as predicated chat rooms. Additionally, if the local user does not know a person's handle but knows his/her email address, said user can invite the known email account user via the "hello" options. Lastly, another option to obtain handles or emails of other users to trade with is through an introduction. The local user can click on the "Friend" drop down menu and select, "Introduce friend". A pop up message will be sent to the two individuals being introduced to each other by the user making the introduction.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

21. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This

sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

22. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating

systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

23. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

24. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

25. Affiant has been informed that FBI Supervisory Special Agent (SSA) James T. Clemente has worked in the Behavioral Analysis Unit of the FBI since 1998. SSA Clemente has been a special agent with the FBI since 1987. As a member of the Behavioral Analysis Unit, SSA Clemente consults on child exploitation cases throughout the United States, South America, and certain European and African countries. Since 1998, he has received three Exceptional Performance Awards from the Department of Justice and a Superior Service Award from the FBI. In addition, he has received numerous letters of commendation from

state, federal, and local law enforcement in connection with his work in the Behavioral Analysis Unit.

26. SSA Clemente's training has involved a significant number of specialized courses in the area of child exploitation, including, but not limited to the following: Innocent Images On-Line Sex Crimes Against Children; National Crimes Against Children; On-Line Sex Crimes Against Children; Clinical Forensic Psychology; Behavioral Analysis of Violent Crime; Missing and Exploited Children Seminar; Research Methodologies; MO, Ritual & Signature Advanced Seminar; and Criminology. In addition, he has mentored under, worked with, studied the articles of, and taught with Kenneth V. Lanning, a Supervisory Special Agent, FBI (retired as of October, 2000). SSA Lanning has over the past 27 years authored numerous articles on the topic of sexual victimization of children and behavioral analysis of child molesters. His work forms the basis of the behavioral analysis performed by the FBI in child exploitation cases.

27. SSA Clemente has assisted in the writing of numerous search warrant affidavits and has testified as an expert witness in federal court in the areas of child sex offender behavior, child sexual victimology and child pornography. He has given over 100 presentations and lectures to local, state and federal law enforcement agencies, prosecutors, and health care professionals throughout the United States on various topics

related to child exploitation, including, but not limited to the following topics: Behavioral Analysis of Child Sex Crimes Offenders, On-Line Sex Crimes Against Children, and Equivocal Death Investigations.

28. As a member of the Behavioral Analysis Unit, SSA Clemente has analyzed and consulted on between one and two hundred child sexual exploitation and victimization cases a year. His analyses are based on all available evidence, including chat records, image collection analysis, collection themes, possession of erotica, possession of sexual paraphernalia, fantasy literature and writings, other relevant acts, and background information. The vast majority of the cases he has analyzed have involved either Preferential or Situational Sex Offenders. His role in these cases has varied as follows: analyzing investigative results for the purpose of making investigative suggestions, providing expert affidavits for search warrant applications, providing interview strategies for subjects and victims, consulting with local, state and federal prosecutors on trial strategies. In addition, SSA Clemente has interviewed between 80 and 100 offenders himself. A behavioral assessment is not a clinical diagnosis; rather, it is a law enforcement tool used to identify and predict offender behavior.

29. SSA Clemente advises of the following traits and characteristics that are generally found to exist and be true in cases involving individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-

based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit

materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.

BACKGROUND OF THE HOUSTON INVESTIGATION

30. In January 2005, an Undercover Officer (UCO) in the Criminal Investigative Division in Media, Pennsylvania, was in the YAHOO! chatroom "PRETEEN Forced and Molested". While in the chatroom the UCO was contacted via YAHOO! Instant Messenger by YAHOO! user "Rayofuva". During the conversation, Rayofuva sent an instant message (IM) containing a link to a photo sharing program called "Hello" to the UCO. Rayofuva told the UCO that "Hello" allows for the transmission of large numbers of pictures quickly. Subsequently, Rayofuva sent the UCO three (3) pictures of what appeared to be child pornography.

31. During the next two months, the UCO and Rayofuva participated in several IM chats. Over the course of those chats, Rayofuva sent the UCO approximately 1000 pornographic images, including more than 680 child pornography images. Additionally, Rayofuva sent seven (7) pornographic movies, six (6) of which were child pornography.

32. Ultimately, Rayofuva was identified as Denzial Tittle, [redacted], Houston, Texas, date of birth: [redacted]. A search warrant was executed at the residence of Tittle, and four computers were seized. A review of one of the computers found at the residence revealed over 8,600 images and 59 movies of child

pornography. A large amount of child pornography images and movies contained on the computer were obtained via the "hello" program from other "hello" users.

33. An administrative subpoena was issued to Google for user account information and IP address login information for the "hello" users communicating with Tittle, which revealed Google User ID: 1161777 which correlated to Google Handle: "dadnkidz". An administrative subpoena for Google Handle "dadnkidz" returned the email address: cranky102@hotmail.com. The search of Tittle's computer indicated receipt of child pornography pictures from Google Handle "dadnkidz" on July 10, 2006 at 06:36:22 EDT. Google, Incorporated, advised that the IP Address assigned to User Handle "dadnkidz" at the aforementioned date and time was 71.200.36.169. According to the results of an Administrative Subpoena to Comcast, IP Address 71.200.36.169 used on July 10, 2006 at 06:36:22 EDT revealed the following subscriber information: Subscriber Name: Scott Robinson; Address: [redacted], Camden, Delaware 19934 (subscriber's service address); Telephone: [redacted] Type of Service: Residential high speed internet service; Account Status: Active; IP Assignment: Dynamically assigned; Account Created: 02/14/2001; Account Number: 0953443790402; E-mail User Ids: csandj3@comcast.net.

34. The examination of Tittle's computer revealed more than 800 images and one video depicting child pornography received

from "hello" user "dadnkidz". Your affiant has reviewed all of the images and the video, and describes fives images as follows:

a. [redacted].jpg (adult man performing oral sex on a prepubescent female)

b. [redacted].jpg (prepubescent boy masturbating an adult male)

c. [redacted].jpg (adult male performing anal sex on a prepubescent boy)

d. [redacted].jpg (baby boy performing oral sex on an adult male)

e. [redacted] (adult male performing sex on a prepubescent boy)

BACKGROUND OF THE INDIANAPOLIS INVESTIGATION

35. FBI - Indianapolis is currently conducting an investigation involving the trading of child pornography between JERRY A. BROWDER, and Indiana resident currently under federal indictment in the Southern District of Indiana, and KENNETH WAYNE MILLER, of [redacted] Iron River, Michigan.

36. On 07/27/2006, FBI-Indianapolis' Innocent Images Unit received information from the Queenland Police Service, Internet Child Exploitation Unit, regarding contact officers had online with an individual, later determined to be BROWDER. During said investigation, BROWDER engaged in online discussions via the Picasa chat program "Hello" with detectives from several jurisdictions utilizing covert identities. "Hello" allows its

users to share files as well as chat. Ultimately, BROWDER transmitted over 100 images of child pornography. From those pictures, the Child Victim Identification Program (CVIP) identified 11 images as from 7 known series. Moreover, during BROWDER's chats, he indicated that he had a 5 year old step-daughter and 9 month old daughter whom he sexually abused.

37. FBI - Indianapolis executed a search warrant at BROWDER's home. A forensic examination of BROWDER's computer was conducted in order to determine if other persons were trading child pornography with BROWDER. In the process, forensic evidence indicated that BROWDER traded child pornography files through the Internet via the "Hello" program with user identification number **1161777**. Subpoenas served upon Hotmail - MSN and Comcast revealed that user number **1161777** indicated the following: handle name - **Dadnkidz**; email address - **cranky102@hotmail.com**; Comcast subscriber - SCOTT ROBINSON , [redacted], Camden-Wyoming, Delaware 19934.

38. FBI - Indianapolis with the assistance of Indiana State Police (ISP) recovered a "Hello" chat log related to the trading activity between BROWDER and **Dadnkidz** (ROBINSON) as well as over 900 visual depictions of minors engaging in sexually explicit conduct, including very young and prepubescent children. Within the 900 images sent by **Dadnkidz** (ROBINSON), approximately 7 images were categorized by the forensic examiner as depicting

sexual violence. Your affiant has reviewed all of the images and describes fives images as follows:

a. [redacted].jpg (infant performing oral sex on an adult male)

b. [redacted].jpg (toddler boy performing oral sex on an adult male)

c. [redacted].jpg (prepubescent girl performing oral sex on an adult male)

d. [redacted].jpg (prepubescent girl with seamen in her mouth pictured with two naked males with their penis' exposed)

e. [redacted].jpg (prepubescent girl performing oral sex on an adult male)

39. a. The FBI has searched various record databases for information about Scott Robinson. Delaware State Department of Motor Vehicles' records, both vehicle and drivers licence, for Scott Robinson indicated an address of [redacted] Camden, Delaware 19934.

b. On January 30, 2007, a request was issued to the United States Postal Inspection Service requesting mailing information for [redacted], Camden, Delaware 19934. The results of the request verified that mail is being delivered to Scott Robinson, [redacted] Robinson, and [redacted] at [redacted], Camden, Delaware 19934.

40. On January 31, 2007, Affiant observed the residence located at [redacted], Camden, Delaware 19934, and it is accurately described in paragraph 37 below.

DESCRIPTION OF THE PREMISES TO BE SEARCHED

41. The location of [redacted], Camden, Delaware 19934, can be described as a two-story home with sand-colored siding, green shutters, two-car garage, small front porch, partial stone front, and an open back yard.

CONCLUSION

42. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that an individual at the Premises has been and is involved in transmitting child pornography. Your Affiant respectfully submits that there is probable cause to believe that at the Premises an individual has violated 18 U.S.C. §§ 2252 and 2252A. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2225A, is located in the Premises, and this evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

43. Your Affiant, therefore, respectfully requests that a warrant be issued authorizing the search and seizure of the items listed in Attachment B.

SA Taneka S. Harris, FBI

Sworn and subscribed before me
this 9 day of February

Honorable Mary Pat Thynge
UNITED STATES MAGISTRATE JUDGE